PLAIN LANGUAGE SERIES — SHANNONGUIDES

The Plain Language Guide to Digital *Privacy.*

No prior knowledge required. No assumptions made. Plain language, straight answers, real experience.

MATT SHANNON
SHANNONGUIDES.COM

MAY 2026
FIRST EDITION

PUBLICATION INFORMATION

The Plain Language Guide to Digital Privacy

Part of the Plain Language Series from ShannonGuides.

Written by Matt Shannon — first edition, May 2026.

How the Guides Fit Together

THE SHANNONGUIDES PLAIN LANGUAGE SERIES

This guide is one of a connected series. Each stands on its own, but together they cover privacy, security, and taking control of your digital life — in the same plain, jargon-free language. If you have this guide, here is how it relates to the others, so you know where to turn for what.

The Plain Language Guide to Digital Privacy — *This guide. The practical foundation for everyone.* The everyday baseline: private messaging, browser and tracker protection, email and aliases, passwords and two-factor authentication, phone settings, data brokers, social media, financial privacy, and smart devices. No technical commitment required. If you are new to all of this, you are in the right place — start here.

The Plain Language Guide to Online OPSEC — *The human layer.* The behaviour, judgment, and habits that decide whether the tools in this guide actually protect you: threat modelling, compartmentalization, identity separation, avoiding the slips that undo your defences. This guide gives you the tools; that one gives you the discipline to use them well.

Escaping Google: The Plain Language Guide — *Leaving one company's ecosystem.* A focused, step-by-step migration off Google's services — email, search, browser, storage, photos, documents, maps, calendar, and the phone itself. The deep treatment of breaking free from a single dominant provider.

The Plain Language Guide to Browser Privacy — *Browser privacy in depth.* The detailed treatment of the browser layer this guide touches on: hardened browsers, tracker and fingerprint defence, private search, and the few habits that make it all work.

The Plain Language Guide to Encrypted Communications — *Private conversation in depth.* The detailed treatment of secure messaging this guide introduces — Signal, encrypted email, the metadata problem, choosing the right tool for the conversation, and using it well.

The Plain Language Guide to Data Broker Removal — *Cleaning up the existing profile.* The detailed treatment of the data-broker exposure this guide briefly addresses — the major brokers, opt-out processes, automated services, your legal rights, and reducing future exposure.

The Plain Language Guide to GrapheneOS — *A private phone.* The deep treatment of the de-Googled phone option this guide mentions — installation, the Google question, daily living with it, and trade-offs honestly named.

The Plain Language Guide to Home Network Privacy — *Network-level privacy.* The detailed treatment of the home network — DNS, ad-blocking at the chokepoint, device segmentation, and the foundations of a private network this guide assumes.

The Plain Language Guides to the Privacy Stack, Self-Hosting, Cryptocurrency Privacy, Financial Privacy, Encrypted Backups, Linux & Unix, Mac & Windows Privacy Hardening, Pseudonymous Online Presence, Workplace Privacy, Children & Family Privacy, Travel OPSEC, and Whistleblower & Journalist Privacy — *The wider catalog.* Advanced compartmentalized computing, running your own services, private money, private money in depth, backing up safely, the foundation operating systems, hardening commercial OSes, pseudonymity, work-life privacy, families and children, travel, and high-stakes situations.

Where this guide fits: Digital Privacy is the starting point for almost everyone. It is the foundation that the other guides build on, extend, or apply to specific domains — but it stands fully on its own and gives most readers the great majority of what they need. If you read no other guide, this one will significantly improve your privacy. If you read others afterwards, you will find this guide's foundations referenced throughout.

The principle uniting the series: privacy is not secrecy or having something to hide — it is *control*, the ordinary human right to decide who knows what about you. Each guide hands you more of that control.

SHANNONGUIDES — PLAIN LANGUAGE SERIES — SHANNONGUIDES.COM

— CONTENTS

Table of *contents.*

CHAPTER 1

What Digital Privacy Actually Means

Before You Begin

This guide is for ordinary people who want more control over their personal information, without needing to become a technical expert or change their entire lives. You do not need any special knowledge to use it. Every term is explained the first time it appears. Every recommendation comes with the reasoning behind it, so you understand not just what to do but why.

Unlike a guide that asks you to install a specialised operating system or rebuild your computer, this guide is about practical, everyday privacy — the changes any person can make on the devices they already own, fitted into the life they already live. Some changes take two minutes. Some take an afternoon. You can do them in any order, as many or as few as you like. Every single one leaves you better protected than before.

The goal is not perfection. The goal is to take back meaningful control over who knows what about you — and to do it in a way that is sustainable, that fits real life, and that you will actually keep up.

What "Privacy" Means — And What It Does Not

Let us clear up the most common misunderstanding right away. Privacy is not secrecy. Privacy is not about having something to hide. Privacy is about *control* — the ability to decide who gets to know what about you, and when.

You draw the curtains at night not because you are doing something shameful, but because what happens in your home is nobody else's business by default. You seal letters in envelopes not because they contain crimes, but because the contents are between you and the recipient. You close the door when you use the bathroom. None of this is secrecy in any sinister sense. It is the ordinary, healthy human expectation that you control your own personal sphere.

Digital privacy is exactly the same expectation, applied to your digital life. It is the right to send a message without a company reading it, to read about a medical symptom without it being logged and sold, to go about your day without your every movement being recorded. When people say "I have nothing to hide," they have misunderstood the question. Privacy is not about hiding. It is about not being required to expose everything to everyone simply because you used a phone or a computer.

What Is Actually Happening to Your Information

To know why these changes matter, it helps to understand what is happening to your personal information right now, as you go about an ordinary day.

You are being tracked across the web. Most websites contain invisible trackers — small pieces of code, often from advertising companies, that record that you visited, what you looked at, and tie it to a profile of you. These trackers follow you from site to site. By the time you have browsed for an hour, dozens of companies you have never heard of may have recorded your activity.

Your data is being bought and sold. There is an entire industry of companies called data brokers whose business is collecting personal information about you — your name, address, phone number, age, income, family, interests, purchases, and much more — and selling it. You never agreed to this directly. They assemble it from public records, from apps, from loyalty cards, from other companies, and they sell it to anyone willing to pay. Most people have never heard of these companies, yet they hold detailed files on nearly everyone.

Your apps are collecting more than they need. A flashlight app does not need your location. A simple game does not need your contacts. Yet many apps request — and receive — far more access to your phone and your data than their function requires, and quietly send that information back to their makers and to advertisers.

Your communications may be readable. Standard text messages and many messaging apps do not fully protect your conversations. The contents, or at least the record of who you talked to and when, may be accessible to the companies involved and to others.

Your devices report on you. Your phone, your smart TV, your voice assistant, your "smart" devices — many of them continuously collect information about how you use them and send it back to their manufacturers.

None of this requires you to have done anything wrong. It happens to everyone, by default, simply as a consequence of using ordinary modern technology. This guide shows you how to switch much of it off.

The Idea of a "Threat Model"

Before changing anything, it is worth spending a moment on one simple, powerful idea that security professionals use: the **threat model**.

A threat model is just an honest answer to two questions: *What am I trying to protect, and who am I protecting it from?*

The answer is different for different people, and that is exactly the point. Consider:

- An ordinary person who simply does not want to be profiled and advertised to, and does not want their data sold, has one threat model.
- A person going through a difficult divorce, who does not want an ex-partner finding their location, has another.
- A nurse, teacher, or public-facing professional who does not want clients or strangers finding their home address has another.
- A journalist protecting a confidential source has a very demanding one.

You do not need the same precautions as an investigative journalist to dramatically improve your everyday privacy. Knowing your own threat model keeps you from two opposite mistakes: doing too little because you feel overwhelmed, or doing so much that it becomes exhausting and you give up.

As you go through this guide, keep your own situation in mind. Take the steps that make sense for your life. Every step is a real improvement, and you can always do more later.

If You Do Nothing Else — The Five Quick Wins

This guide is thorough, but you do not have to do all of it to benefit enormously. If you only ever make five changes, make these — they deliver the large majority of the benefit for a small fraction of the effort:

1. **Install a password manager** and give your most important accounts strong, unique passwords (Chapter 5). This single step protects you against the most common way ordinary accounts are compromised.
2. **Turn on two-factor authentication** for your email and other important accounts (Chapter 5). A second lock that stops most account takeovers cold.
3. **Switch to a private browser with uBlock Origin** — Firefox or Brave (Chapter 3). Stops most of the tracking that follows you across the web.
4. **Move your real conversations to Signal** (Chapter 2). Protects your most personal communications with almost no effort.
5. **Set your peer-to-peer payment apps to private and audit your phone's app permissions** (Chapters 9 and 6). Closes two of the widest, least-known data leaks in a couple of minutes.

If you do only these five, you will already be far ahead of where most people stand. Everything else in this guide builds further protection on top of this foundation. Do the rest at your own pace.

How This Guide Is Organised

This guide moves from the changes that affect the most people to the more specialised. You can follow it in order, or jump to whatever concerns you most.

- **Private messaging** — protecting your conversations
- **Browser and tracker protection** — stopping the web from following you
- **Email privacy and aliases** — protecting your inbox and your identity
- **Passwords and account security** — locking down access
- **Your phone's privacy settings** — taming the device that knows the most
- **Data broker removal** — getting your information off the market

- **Social media privacy** — controlling what you expose
- **Financial privacy** — protecting your spending and identity
- **Smart devices and the home** — handling the internet of things
- **Putting it all together** — building habits that last

Each chapter explains why the topic matters, gives you clear recommendations with alternatives, walks you through the steps, and ends with a summary.

A Realistic Promise

You will not finish this guide invisible, and that is not the goal. Total invisibility is neither achievable nor necessary for an ordinary person living an ordinary life. What you *will* achieve is this: dramatically less tracking, far less of your data on the open market, private conversations, secure accounts, and meaningful control over your personal information. You will be a vastly harder target for advertisers, data brokers, scammers, and casual snoops — and you will understand your own digital life well enough to keep it that way.

That is a realistic, achievable, and genuinely valuable goal. Let us begin.

Chapter Summary

Privacy is not secrecy or having something to hide — it is control over who knows what about you, the same ordinary expectation behind curtains, envelopes, and closed doors. Right now, by default, you are tracked across the web, your data is bought and sold by brokers, your apps over-collect, and your devices report on you — none of which requires any wrongdoing on your part. The idea of a threat model — knowing what you are protecting and from whom — helps you take the right amount of action for your life. This guide moves from the most universal changes to the more specialised, and the goal is not invisibility but meaningful, sustainable control.

The next chapter begins with the conversations you have every day: private messaging.

Chapter 2: Private Messaging →

CHAPTER 2

Private Messaging

Why Your Conversations Need Protecting

Think about what you say in your messages over a single week. Plans with family. Money matters. Health updates. Frustrations about work. Photos of your children. Things you would say to a trusted friend but to no one else. Now consider that with ordinary text messages and many popular apps, those conversations are not fully private — the company carrying them, and potentially others, can read the contents or at least keep a detailed record of who you talked to, when, and how often.

Your conversations are some of the most personal data you generate. This chapter shows you how to protect them, and the good news is that it is one of the easier changes to make — the tools are free, excellent, and easy to use.

Understanding the Two Things That Need Protecting

When it comes to private messaging, there are two separate things to protect, and understanding the difference helps you choose the right tool.

The content of your messages — the actual words, photos, and files you send. This is protected by something called **end-to-end encryption**, which means your message is scrambled on your device and can only be unscrambled by the person you sent it to. The company in the middle carries only the scrambled version, which it cannot read. This is the single most important feature to look for.

The metadata — the record *around* your messages: who you talked to, when, how often, and from where. Metadata sounds harmless, but it is extraordinarily revealing. A former head of the American National Security Agency once said plainly that governments act on the basis of metadata. Knowing that you called a particular doctor, then a family member, then a support line, late at night, reveals a great deal even if no one read a single word. The most private messengers protect metadata as well as content.

Different apps protect these to different degrees, which is the basis for the recommendations below.

The Recommended Choice: Signal

For almost everyone, the right choice is **Signal**.

Signal is a free, independent messaging app run by a non-profit foundation. It is widely regarded by security experts as the gold standard for private messaging that ordinary people can actually use, and it is what the privacy community overwhelmingly recommends.

Why Signal:

- **Best-in-class end-to-end encryption.** Signal's encryption is so well-regarded that other major apps licensed and copied it. It is the gold standard, and everything — messages, calls, video, photos — is encrypted.
- **It collects almost nothing about you.** Signal is designed to hold as little information as possible. When legally compelled to hand over data, Signal has been able to provide almost nothing, because it simply does not collect it.
- **It is free and non-profit.** There is no advertising business behind it, no incentive to harvest your data. It is funded by donations and grants.
- **It is easy to use.** It works almost exactly like the messaging apps you already know. Messages, group chats, voice and video calls, photos, voice notes — all there, all familiar.
- **It is genuinely private by default.** You do not need to change settings or understand encryption. It just works, privately, out of the box.

The one catch: Signal requires a phone number to register. This means the people you talk to can know your number (though you can now use a separate username to connect without sharing your number directly). For the vast majority of people, this is a perfectly acceptable trade for an app that is both genuinely private and easy enough that your friends and family will actually use it.

The most important factor of all: A private messenger is only useful if the people you want to talk to also use it. Signal's great advantage is that it is popular enough, and easy enough, that you can realistically get your contacts onto it. The most secure app in the world is useless if you are the only person on it.

Alternatives

SimpleX Chat — For those who want the maximum possible privacy, SimpleX is remarkable: it uses no user identifiers at all — no phone number, no email, no account ID. Because of how it is built, its servers cannot even know who is talking to whom, giving the strongest metadata protection available. The tradeoffs are that it is younger and less battle-tested than Signal, and its user base is small, so you will likely have to convince contacts to join. The best choice when anonymity is paramount.

Threema — A Swiss app that does not require a phone number or email to use; you are identified only by an anonymous ID. It offers strong metadata protection and the benefit of Swiss privacy law. It costs a small one-time fee to buy, which some people actually prefer — you are clearly the customer, not the product. A great choice for the privacy-conscious, especially in Europe.

Molly — A version of Signal, hardened with extra security features, for Android users who want Signal's network and usability with additional protection.

Briar — A specialised app for high-risk situations that can even work without the internet, connecting devices directly. Niche, aimed at activists and journalists in extreme circumstances, but worth knowing exists.

A note on WhatsApp: WhatsApp does use Signal's encryption for message contents, which is genuinely good. But it is owned by Meta (Facebook), which collects extensive metadata about who you talk to and when, and ties it to your broader profile. It is far better than unencrypted texting, but it is not a private choice in the fuller sense. If you currently use WhatsApp, moving to Signal is a clear upgrade.

A note on Telegram: Despite its privacy reputation, Telegram's chats are *not* end-to-end encrypted by default — only special "secret chats" are. Ordinary Telegram messages are readable by Telegram. It is not recommended as a private messenger.

For most people, the path is simple: **use Signal**, and reach for SimpleX or Threema if your situation calls for stronger anonymity.

Step 1: Install Signal

1. On your phone, install Signal from your app store (the Apple App Store or, on Android, the Play Store or a private store as covered in the phone chapter)
2. Open it and follow the prompts to register with your phone number
3. Verify your number with the code Signal sends you
4. Set up your profile — you can add a name and photo, which only your contacts see

You can also install Signal on your computer (from signal.org) and link it to your phone, so you can message from your desktop too.

Step 2: Set a Username to Protect Your Phone Number

Signal now lets you create a username so you can connect with people without giving out your phone number:

1. In Signal, go to **Settings → Profile**
2. Set up a **username**
3. You can now share your username instead of your number, and adjust the privacy settings so your number is not visible to people who only have your username

This is useful if you want to message someone without exposing your personal phone number.

Step 3: Turn On Disappearing Messages (Optional)

Signal can automatically delete messages after a set time — a day, a week, whatever you choose. This means old conversations do not pile up indefinitely on either device.

1. Open a conversation
2. Tap the contact's name at the top
3. Find **Disappearing Messages** and choose a timer
4. You can also set a default timer for all new conversations in Settings → Privacy

This is a good habit: it limits how much sensitive history sits on your phone, where it could be exposed if your phone is lost or seized.

Step 4: Bring Your People With You

The hardest part of private messaging is social, not technical. Here is how to make the switch stick:

- Tell the people you message most that you are moving to Signal, and why, in simple terms: "It's free, it's more private, and it works just like what we use now."
- Start using Signal as your default for the people who are on it
- Be patient and gently persistent — as more of your contacts join, the easier it becomes
- Lead by example: when someone asks for your number, offer Signal

You do not have to convert everyone overnight. Even moving your most personal conversations — family, close friends, anything sensitive — to Signal is a major gain, even if some casual contacts stay on other platforms for a while.

A Note on Texts You Cannot Move

You will not be able to move everyone to a private messenger, and some messages — like verification codes from businesses, or texts from people who will never switch — will keep coming through ordinary channels. That is fine. The goal is to protect your real conversations, especially the personal and sensitive ones. Standard texts for impersonal purposes are a smaller concern. Protect what matters most first.

Chapter Summary

Your conversations are among your most personal data, and ordinary texts and many popular apps do not fully protect them — either the content or the revealing metadata around them. Signal is the recommended choice for nearly everyone: best-in-class encryption, almost no data collected, free, non-profit, and easy enough that your contacts will actually use it. SimpleX and Threema offer even stronger anonymity for those who need it, while WhatsApp

and Telegram fall short for different reasons. You installed Signal, optionally set a username to protect your phone number, enabled disappearing messages, and began bringing your contacts along.

The next chapter tackles the thing following you everywhere you go online: web trackers.

Chapter 3: Browser and Tracker Protection →

CHAPTER 3

Browser and Tracker Protection

The Invisible Followers

Every time you visit a website, you are rarely dealing with just that one website. Hidden inside most web pages are trackers — small pieces of code, usually belonging to advertising and data companies, that quietly record your visit. They note what page you are on, what you look at, how long you stay, and they tie this to a profile that follows you from site to site across the internet.

This is how it happens that you look at a product once and then see advertisements for it everywhere for weeks. It is not a coincidence and it is not your imagination. You are being followed, continuously, by companies you have never heard of and never agreed to deal with. This chapter shows you how to switch off most of that tracking — and like private messaging, it is one of the higher-impact, lower-effort changes you can make.

How Web Tracking Actually Works

Understanding the basic mechanics makes the solutions obvious.

Third-party trackers. When you visit a news site, the page may load content from dozens of other companies — ad networks, analytics firms, social media widgets. Each of these can drop a marker on your device and record your visit. Because the same tracking companies have code on thousands of sites, they can stitch together a picture of your browsing across the whole web.

Cookies. A cookie is a small file a website stores on your device to remember you. Some cookies are useful and harmless — remembering you are logged in, keeping items in a shopping cart. Others, called third-party tracking cookies, exist purely to follow you around and build an advertising profile.

Browser fingerprinting. This is subtler. Your browser reveals small details about your device — your screen size, your fonts, your settings, your time zone. Combined, these details can

form a “fingerprint” unique enough to recognise you even without cookies. It is a sneakier form of tracking that good privacy tools also resist. Firefox and Brave both include fingerprinting resistance, and for those who want the strongest protection, specialised browsers built for this exist — **Mullvad Browser** and **LibreWolf** are both designed to make you look identical to other users, defeating fingerprinting. These are excellent for advanced users, though they intentionally strip away conveniences (saved logins, history) that make them less suited to everyday use.

Your search engine. As covered in the privacy world generally, your search engine sees everything you search for. If it is one that profiles you, that is a major stream of personal information.

The defences against all of these are the same handful of changes below.

Step One: Choose a Private Browser

Your browser is the window through which you experience the web — and through which the web observes you. The browser you use matters enormously.

The Recommended Choices: Firefox or Brave

Mozilla Firefox is made by a non-profit and runs on its own independent engine, which is good for the health of the web. With a few settings changes it becomes very private, and it fully supports the most powerful privacy add-on (uBlock Origin).

Brave is built for privacy out of the box — it blocks ads and trackers automatically with no setup, and it is built on the same underlying engine as Chrome, so it feels familiar and runs Chrome’s add-ons.

Either is an excellent choice. Choose **Firefox** to support an independent web and do a few minutes of setup; choose **Brave** for privacy with essentially zero configuration. Both are free.

What to move away from: Google Chrome (built by an advertising company to feed your activity into your profile) and Microsoft Edge (similar concerns). If you use either as your main browser, switching is one of the most valuable privacy changes available to you.

Install and Set Up

1. Download Firefox from **mozilla.org/firefox** or Brave from **brave.com**

2. Install it and allow it to import your bookmarks from your old browser
3. Set it as your default browser in your computer's or phone's settings so links open in it automatically

---

Step Two: Harden Firefox (If You Chose Firefox)

Brave is already locked down by default, so Brave users can skip to Step Three. If you chose Firefox, these quick changes raise your protection substantially:

1. Open Firefox **Settings → Privacy & Security**
2. Under **Enhanced Tracking Protection**, choose **Strict** — this blocks far more trackers
3. Turn on the option to send websites a **"Do Not Track"** request, and the **Global Privacy Control** signal if present
4. Consider setting cookies to clear when you close Firefox (you will be logged out of sites each session, which is a small tradeoff for more privacy)
5. Turn off Firefox's optional data collection if you prefer Mozilla receive nothing

These take two minutes and meaningfully reduce tracking.

Step Three: Install uBlock Origin

This is the single most effective privacy tool you can add to a browser. **uBlock Origin** is a free, open-source content blocker that stops ads and trackers across the entire web. It dramatically reduces the companies able to follow you, and as a bonus, pages load faster and cleaner.

Important: uBlock Origin works fully in **Firefox** and **Brave**. It does *not* work properly in Chrome any longer, because Google changed Chrome's rules in ways that cripple it — one more reason to leave Chrome. (Brave has its own strong blocking built in, so uBlock Origin is optional there, but Firefox users should absolutely install it.)

To install in Firefox:

1. Go to **addons.mozilla.org**
2. Search for **uBlock Origin**

3. Click **Add to Firefox** and confirm
4. The shield icon appears in your toolbar — it now works automatically, blocking trackers and ads on every site

You do not need to configure anything. uBlock Origin works well out of the box.

Step Four: Set a Private Search Engine

Your search engine sees every search you make. Replace a tracking search engine with a private one. This takes two minutes and stops one of the largest streams of personal information about you.

The Recommended Choice: Brave Search

Brave Search has its own independent index of the web, does not track or profile you, requires no account, and returns good-quality results for everyday searching. It works in any browser. (The companion guide *Escaping Google* covers private search engines in more depth in its own dedicated chapter, if you want the fuller treatment.)

Alternatives

- **DuckDuckGo** — The best-known private search engine, easy and reliable, with a clean interface.
- **Startpage** — Delivers Google's results through a privacy shield, so you get Google-quality results without Google tracking you. Best if you specifically want Google-style results.
- **Mojeek** — A genuinely independent search engine for those who want maximum independence from the big players.

Set It as Default

In your browser's settings, find the search section and set your chosen engine as the default. In Brave, Brave Search is a built-in option. In Firefox, go to **Settings → Search** and choose it (you may need to visit the search engine's site once first so it appears).

Step Five: A Few More Useful Habits

Use private/incognito windows for sensitive searches. A private window does not save history or cookies after you close it. It is not invisible to your internet provider, but it keeps sensitive browsing off your device and out of your normal cookie profile.

Be cautious with browser extensions. Add-ons can be powerful, but a malicious or careless extension can spy on your browsing. Install only well-known, reputable extensions like uBlock Origin, and keep the number small. Each extension is a potential risk.

Log out of accounts when not using them. When you are logged into a big platform — especially a social media or Google account — while browsing other sites, that platform can more easily tie your wider browsing to your identity. Logging out helps break that link.

Consider a separate browser for your most-tracked accounts. Some people use one browser for logged-in accounts (social media, shopping) and a different one for general browsing, keeping the two worlds separate so the trackers cannot easily connect them.

Understanding VPNs — What They Do and Do Not Do

You have almost certainly seen VPNs advertised heavily as a privacy must-have. The advertising oversells them, but a VPN is a genuinely useful tool when you understand exactly what it does — and, just as importantly, what it does not do.

What a VPN is. A VPN (Virtual Private Network) creates an encrypted tunnel between your device and a server run by the VPN provider. Your internet traffic travels through that tunnel before reaching the wider internet. This has two effects: the websites you visit see the VPN server's location and address instead of your real one, and your internet provider (or the operator of a public Wi-Fi network) can no longer see which sites you are visiting — only that you are connected to a VPN.

What a VPN is genuinely good for:

- **Public Wi-Fi.** On the open Wi-Fi of a café, airport, or hotel, a VPN protects your traffic from others on the same network. This is one of its strongest, clearest uses.

- **Hiding your browsing from your internet provider.** Your provider can otherwise see and log every site you visit; a VPN prevents this.
- **Hiding your real location/address from websites**, which adds a layer of privacy and can reduce location-based profiling.

What a VPN does NOT do — this is the crucial part the advertising hides:

- It does **not** stop the web trackers, cookies, and fingerprinting covered in this chapter. Those follow you regardless of your VPN. The browser protections above matter *more* for everyday tracking than a VPN does.
- It does **not** make you anonymous. The VPN provider can see your traffic, which is why *who* you trust as your provider is everything.
- It does **not** protect you if you are logged into accounts that identify you — your VPN does not hide who you are from a site you have signed into.

The most important rule: never use a free VPN. Running a VPN costs the provider real money. A free VPN has to make that money somehow, and the answer is almost always by logging and selling the very traffic you used it to protect. A free VPN is often worse for your privacy than no VPN at all. This is one of the clearest rules in all of digital privacy.

Choosing a VPN. If you want one, choose a reputable, paid, independently-audited, no-logs provider. The two most respected choices are:

- **Proton VPN** — part of the Proton ecosystem referenced throughout this series, with a genuinely usable (and trustworthy) free tier, which is a rare exception to the free-VPN rule because Proton's business is funded by paid subscriptions rather than by selling data.
- **Mullvad** — known for requiring no account or email, accepting anonymous payment, and a strongly verified no-logs record.

Do you need one? For most people, a VPN is worth having for public Wi-Fi and to keep your browsing from your internet provider — but it is a complement to, not a substitute for, the browser protections in this chapter. Set up your private browser, uBlock Origin, and private search first; add a reputable paid VPN if the uses above matter to you.

Chapter Summary

Most websites carry hidden trackers that follow you across the internet, building advertising profiles through third-party trackers, tracking cookies, and browser fingerprinting. The defences are straightforward and high-impact: switch to a private browser (Firefox or Brave), harden Firefox's settings if you chose it, install uBlock Origin (the single most effective privacy tool, which Chrome deliberately cripples), and set a private search engine like Brave Search. A few extra habits — private windows, cautious extension use, logging out of big accounts — round it out. A VPN is a useful but separate tool that addresses a different problem.

The next chapter protects your inbox and one of the most powerful privacy tools available: the email alias.

Chapter 4: Email Privacy and Aliases →

CHAPTER 4

Email Privacy and Aliases

Your Email Address Is a Tracking Number

Most people have one email address that they use for everything — their bank, their shopping, their social media, every newsletter, every app, every one-time signup. Over the years that single address gets handed out hundreds of times.

This creates two problems. First, your email address becomes a universal identifier that links all your accounts together. When a company buys data about you, your email address is often the key that connects the pieces — the same address at your bank, your pharmacy, and your favourite shop lets data brokers stitch your activity into one profile. Second, when any one of those hundreds of companies suffers a data breach — and they do, constantly — your address leaks, leading to spam, phishing attempts, and your address being sold on.

This chapter addresses both the privacy of your email itself and a powerful technique most people have never heard of: email aliases.

Part One: Private Email

Email is covered in much greater depth in the companion guide *Escaping Google*, which walks through a complete, careful migration from Gmail — importing your old mail, updating hundreds of accounts, forwarding, and safely closing your old address. If full email migration is your goal, that guide is the place to do it thoroughly. Here we cover the essentials and one powerful technique that applies to everyone.

Ordinary email services like Gmail, Outlook, and Yahoo can read the contents of your emails (or could, and certainly store them readably), scan them, and tie them to a profile. The contents of your inbox — which include your most sensitive correspondence — sit on their servers, readable, and accessible to data requests.

The Recommended Choice: Proton Mail

Proton Mail is an encrypted email service based in Switzerland. Your emails are protected with end-to-end encryption, meaning Proton itself cannot read your stored messages. It re-

quires no personal information to sign up, has a capable free tier, and is the most established private email provider.

Alternatives include **Tuta** (German, encrypted, very affordable), **Mailbox.org** and **Mailfence** (full-featured European providers), and **Posteo** (low-cost, ethical, German). Any is a major improvement over a surveillance-funded provider.

You do not necessarily have to abandon your existing email overnight — the *Escaping Google* guide covers a full migration carefully, step by step. But for your sensitive correspondence going forward, a private provider is the foundation. And the Proton ecosystem referenced throughout this series is worth understanding as a whole: a single Proton account provides not just encrypted email but also encrypted calendar, cloud storage, a password manager (Proton Pass), and a VPN — an integrated, privacy-respecting alternative to the all-in-one convenience that Google offers. You do not have to use all of it, but it means the tools in several chapters of this guide can come from one trusted source if you prefer.

Part Two: The Power of Email Aliases

This is the technique that surprises people most, because it is so simple and so effective.

An **email alias** is a disposable, forwarding email address. Instead of giving a company your real email address, you give it a unique alias — a randomly generated address that forwards to your real inbox. You can create a different alias for every service. The company never sees your real address; it only sees the alias.

Why this is so powerful:

- **It breaks the universal identifier.** Because every service has a *different* address for you, your accounts can no longer be linked together by a shared email address. The data brokers lose their key.
- **It reveals who leaked or sold your data.** If you create the alias “shopname@yourdomain” and only ever give it to one shop, and you suddenly receive spam to that exact alias, you know precisely who leaked or sold your address. This is remarkably satisfying and informative.
- **It lets you cut off spam at the source.** If an alias starts receiving spam, you simply disable that one alias. The spam stops instantly, and your real address and all your other aliases are unaffected.

- **It protects your real address from breaches.** When a company is breached, only the alias you gave them is exposed — not your real email, and not your other accounts.

How Aliases Work in Practice

You sign up with an alias service or use one built into your email provider. When you need to give an email address to a new service, you generate a fresh alias — something like `a8f3kd@aliasservice.com` or a custom one like `netflix@yourname.something`. Mail sent to that alias arrives in your normal inbox. You can reply, and it appears to come from the alias. The other party never learns your real address.

The Recommended Choices

Proton Pass aliases — If you use Proton (Mail or the Proton Pass password manager from the password chapter), alias creation is built right in. Proton Pass can generate a "hide-my-email" alias every time you sign up for something, directly in your browser. This is the most seamless option if you are already in the Proton ecosystem.

SimpleLogin — An open-source alias service (now part of Proton) dedicated to this purpose. It lets you generate unlimited aliases, organise them, and manage them easily. Excellent and purpose-built.

addy.io (formerly AnonAddy) — Another excellent open-source alias service, with a generous free tier. A strong independent choice.

Apple's Hide My Email — If you use Apple devices and pay for iCloud+, Apple offers built-in alias creation. Convenient for people already in the Apple ecosystem, though it keeps you tied to Apple.

Step 1: Set Up an Alias Service

1. If you use Proton, explore **Proton Pass** — alias creation is built in; you can generate one whenever a website asks for your email
2. Otherwise, sign up for **SimpleLogin** or **addy.io** (both have free tiers)
3. Install their browser extension, which lets you generate a new alias with one click whenever you encounter a signup form

Step 2: Start Using Aliases for New Signups

You do not need to convert all your existing accounts at once. Going forward, every time you sign up for something new:

1. Generate a fresh alias
2. Use it instead of your real address
3. The service's mail forwards to your normal inbox as usual

Over time, your real address gets handed out less and less, and your new accounts are protected from the start.

Step 3: Migrate High-Value Accounts Gradually

For your most important or most spam-prone existing accounts, you can update them to aliases over time — change the email on the account to a new alias, confirm it works, and your real address is removed from that company's records. Prioritise accounts that send you a lot of marketing or that you do not fully trust.

A Note on "Plus Addressing" (and Why Aliases Are Better)

You may know a trick where you add a "+something" to a Gmail address — like `your-name+shop@gmail.com` — and it still reaches your inbox. This can help you filter mail and spot who shared your address, but it is *not* a privacy tool: anyone can simply delete the "+shop" part to find your real address, and it still exposes your real address to every service. Proper aliases, which are entirely separate addresses, are far more protective. Use real aliases, not plus addressing, when privacy is the goal.

Chapter Summary

Your single email address acts as a universal tracking number that links all your accounts and leaks in every data breach. Protecting your inbox means two things: using a private, encrypted email provider like Proton Mail (with Tuta, Mailbox.org, and others as alternatives), and — the technique most people have never used — email aliases. A unique forwarding alias for each service breaks the universal identifier, reveals exactly who leaked or sold your data, lets

you cut off spam at its source, and shields your real address from breaches. Proton Pass, SimpleLogin, and addy.io make aliases easy. Use them for new signups going forward and migrate high-value accounts over time.

The next chapter locks down the keys to everything: your passwords and account security.

Chapter 5: Passwords and Account Security →

CHAPTER 5

Passwords and Account Security

The Keys to Everything

Every privacy measure in this guide depends on one thing: that the accounts holding your private information stay in your control. The strongest encryption in the world protects nothing if someone simply logs in as you. Your passwords, and the locks on your accounts, are the foundation everything else rests on.

This is also the area where most people are dangerously exposed without realising it — not through any technical attack, but through three ordinary habits that are easy to fix.

The Three Dangerous Habits

Reusing the same password. Most people use the same password, or a few variations, across many accounts. The problem: when any one of those services is breached — and breaches happen constantly — the leaked password is tried automatically against all your other accounts. One breach becomes many. This is, by a wide margin, the most common way ordinary people's accounts are compromised.

Weak, guessable passwords. Passwords based on names, birthdays, pets, or common words and patterns are far easier to crack than people imagine. Automated tools try millions of likely guesses.

Relying on memory. Because remembering many strong unique passwords is impossible, people fall back on reuse and weak choices. The solution is not a better memory — it is to stop relying on memory at all.

All three are solved by one tool.

The Solution: A Password Manager

A **password manager** is a secure, encrypted application whose entire job is to remember your passwords for you. You remember one strong master password; it remembers everything else. It generates long, random, unique passwords for every account — passwords you never need to see or type — and fills them in automatically.

This single tool eliminates all three dangerous habits at once. Every account gets a strong, unique password. A breach at one service exposes nothing about any other. And you no longer have to remember anything but your one master password.

How it works: Your passwords live in an encrypted vault, locked by your master password. The manager has browser extensions and phone apps that recognise login pages and fill in the right credentials. When you create a new account, it offers to generate a strong password and save it automatically.

The one rule that matters most: Your master password must be strong, and it must be unique — never used anywhere else. Because it protects everything, make it a long passphrase you can remember: several random words strung together, like `copper-anchor-velvet-thunder`, are both strong and memorable. Write it down and store it somewhere physically safe, such as a locked drawer at home. If you forget it, your vault cannot be recovered — that is the point of real encryption.

The Recommended Choices

Bitwarden — The most widely recommended password manager. Free, open-source, independently audited, and excellent. Its free tier is genuinely generous — unlimited passwords across all your devices. Works in every browser and on every phone. The best choice for most people.

Proton Pass — If you use the Proton ecosystem (from the email chapter), Proton Pass is built in, end-to-end encrypted, and includes the email alias feature from the previous chapter. The seamless choice if you are already with Proton.

KeePassXC — A completely offline password manager. Your vault is a single encrypted file stored only on your own devices — nothing in anyone's cloud. Maximum control and privacy, with the tradeoff that you manage syncing the file between devices yourself (often by keeping it in your private cloud storage). Favoured by the most privacy-conscious.

Any of these is excellent. **Bitwarden** is the easiest best-in-class choice; **Proton Pass** if you are in the Proton ecosystem; **KeePassXC** for maximum control.

Step 1: Set Up Your Password Manager

1. Sign up for Bitwarden at **bitwarden.com** (or set up Proton Pass, or download KeePassXC)
2. Create your strong master passphrase and store it safely
3. Install the browser extension and the phone app

Step 2: Add Your Accounts Over Time

You do not need to do everything at once:

1. Let the manager save your logins as you sign in to sites normally — within a few weeks it captures most of your accounts
2. As you log in to each important account, change its password to a strong unique one generated by the manager, starting with your most critical accounts (email, bank, anything financial)
3. Use the manager's built-in checker, which flags weak and reused passwords, as a to-do list to work through gradually

---

The Second Lock: Two-Factor Authentication

A password alone is a single lock. **Two-factor authentication** (2FA) adds a second, independent lock, so that even if someone learns your password, they still cannot get in. It is one of the most effective security measures available, and you should turn it on for every important account — especially your email and your password manager.

How 2FA Works

After entering your password, you provide a second proof that it is really you — usually a six-digit code that changes every thirty seconds, generated by an app on your phone. Even if an attacker has your password, they do not have your phone, so they cannot produce the code.

The Right Kind of 2FA

Not all 2FA is equal. In order of preference:

Hardware security keys (most secure). A small physical device (such as a YubiKey) that you plug in or tap to prove it is you. Nearly impossible to defeat remotely. Ideal for your most critical accounts. A small cost, but the strongest protection available.

Authenticator apps (recommended for most). A free app on your phone generates the codes. This is the sweet spot of security and convenience for most people. Recommended apps: **Aegis** (Android), **Ente Auth** (Android and iPhone), or **Proton Authenticator** — all free, open-source, and private.

Avoid text-message (SMS) codes where possible. Receiving 2FA codes by text is better than no 2FA, but it is the weakest form, because phone numbers can be hijacked by a scam called "SIM swapping," where an attacker tricks your phone carrier into transferring your number to them. Use an authenticator app instead of SMS wherever a service allows it.

A note on Google Authenticator: If you currently use Google Authenticator, consider moving to Aegis, Ente Auth, or Proton Authenticator — they offer better privacy and encrypted backups, and they keep you out of Google's ecosystem.

Step 1: Set Up an Authenticator App

1. Install Aegis, Ente Auth, or Proton Authenticator on your phone
2. Enable its encrypted backup so you do not lose your codes if you lose your phone

Step 2: Turn On 2FA for Your Important Accounts

For each important account (start with email and your password manager):

1. Go to the account's security settings
2. Find two-factor authentication and choose the authenticator-app option
3. Scan the QR code with your authenticator app
4. Save the **backup codes** the service gives you in your password manager — these let you back in if you ever lose your phone

Critical: Plan for Losing Your Phone or Authenticator

This is the step people skip, and it causes real misery. If your two-factor codes live only on your phone and you lose that phone, you can be locked out of your own accounts — sometimes permanently. Protect yourself before it happens:

- **Save every account's backup codes.** When you turn on 2FA, the service offers a set of one-time backup codes. Always save them — in your password manager is ideal, since it is encrypted and synced. These codes let you log in if your authenticator is gone.
- **Use an authenticator app with encrypted backup.** Aegis, Ente Auth, and Proton Authenticator all offer encrypted backups of your 2FA codes. Turn this on. It means that if you lose your phone, you can restore all your codes to a new one rather than being locked out of everything at once.
- **Consider a second factor on critical accounts.** For your most important accounts, some services let you register more than one 2FA method — for example, an authenticator app *and* a hardware key, or two hardware keys (one kept safely at home). If one is lost, the other still works.

What to Do If You Lose Your Authenticator

If the worst happens and you lose your phone with your authenticator on it:

- Use your saved **backup codes** to log in to each account and re-establish 2FA on a new device
- If you enabled **encrypted backup** in your authenticator app, simply install the app on your new phone and restore from the backup
- For accounts where you have neither, you will need to go through each service's account-recovery process, which can be slow — which is exactly why saving backup codes in advance matters so much

The lesson: set up your recovery *before* you need it. Saving backup codes and enabling encrypted authenticator backup takes a few minutes and can save you from being locked out of your digital life.

A Word on Data Breaches

Even with perfect habits, companies you deal with will be breached — that is outside your control. Two things help:

Check if you have been breached. The free site **Have I Been Pwned** (haveibeenpwned.com) lets you enter your email address to see whether it has appeared in known data breaches. It is run by a respected security researcher and is safe to use. If your address shows up, change the password on the affected account (and anywhere you reused it — another reason never to reuse).

Aliases limit the damage. As covered in the previous chapter, using a different email alias per service means a breach exposes only that one alias, not your universal address.

Chapter Summary

Your accounts are the foundation that every other privacy measure depends on, and most people are exposed through three ordinary habits: reusing passwords, choosing weak ones, and relying on memory. A password manager — Bitwarden for most, Proton Pass within the Proton ecosystem, or KeePassXC for maximum control — solves all three by generating and remembering strong unique passwords behind one master passphrase. Two-factor authentication adds a critical second lock: use a hardware key for the most important accounts or an authenticator app like Aegis or Ente Auth for everything else, and avoid SMS codes where you can. Checking Have I Been Pwned and using email aliases limit the damage when companies are inevitably breached.

The next chapter turns to the device that knows more about you than any other: your phone.

Chapter 6: Your Phone's Privacy Settings →

CHAPTER 6

Your Phone's Privacy Settings

The Device That Knows You Best

Your phone is with you almost every hour of every day. It knows where you are, who you talk to, what you read, what you buy, when you wake and sleep. It carries your photos, your messages, your location, your habits. Of everything you own, your phone holds the richest picture of your life — and by default, it shares a great deal of that picture with the company that made it, the apps you install, and the advertisers behind them.

This chapter does not ask you to replace your phone or its operating system (that fuller step is covered in the *Escaping Google* guide and a dedicated phone guide). Instead, it shows you how to lock down the phone you already have — meaningful changes anyone can make in an afternoon, on either an iPhone or an Android phone.

The Biggest Lever: App Permissions

The single most valuable thing you can do for phone privacy is to control what your apps are allowed to access. Most apps ask for far more than they need. A flashlight app does not need your location. A photo-editing app does not need your contacts. A simple game does not need your microphone. Yet apps request these permissions routinely, and most people tap "allow" without thinking — and once granted, that access is used to collect and often sell your data.

Going through your permissions and revoking what is unnecessary is the highest-impact phone privacy step. Be ruthless: an app should only have access to what it genuinely needs to do its job.

On iPhone

1. Open **Settings → Privacy & Security**
2. Go through each category — **Location Services**, **Contacts**, **Microphone**, **Camera**, **Photos**, and so on
3. For each, review which apps have access and revoke any that do not need it

4. For **Location Services** especially, set apps to **While Using** rather than **Always**, and turn location off entirely for apps that do not need it
5. For **Photos**, prefer **Limited Access** (selected photos) or **Add Photos Only** over full library access where possible

On Android

1. Open **Settings → Privacy → Permission manager** (wording varies slightly by phone)
2. Go through each permission category and review which apps have access
3. Revoke anything unnecessary
4. For location, choose **Allow only while using the app** rather than all the time, and deny it entirely where it is not needed

Do this for every app. You will be surprised how much access you have granted without realising, and how little most apps actually need.

Turn Off Advertising Tracking

Both iPhone and Android assign your phone an advertising identifier — a unique number used to track you across apps for advertising. You can limit or reset this.

On iPhone

1. **Settings → Privacy & Security → Tracking**
2. Turn off **Allow Apps to Request to Track** — this stops apps from tracking you across other apps and websites. This is Apple's **App Tracking Transparency** feature, and it is genuinely powerful: it forces every app to ask permission before tracking you across other companies' apps and sites, and turning it off here denies them all at once. It is one of the most effective single privacy toggles on any phone.
3. Then **Settings → Privacy & Security → Apple Advertising** and turn off **Personalized Ads**

Two more iPhone privacy features worth using:

- **Hide My Email.** If you subscribe to iCloud+, Apple can generate random email addresses that forward to your real inbox — the same alias concept from Chapter 4, built right into the phone. When an app or website asks for your email, you can hand over a unique Apple-generated address instead of your real one. Find it in your iCloud settings, and it appears automatically on signup screens.

- **iCloud Private Relay.** Also part of iCloud+, this hides your browsing in Safari from your internet provider and the sites you visit, in a way loosely similar to a VPN for Safari. Turn it on in **Settings → [your name] → iCloud → Private Relay**. It is not a full VPN, but it is a meaningful, effortless privacy gain for Apple users.

On Android

1. **Settings → Privacy → Ads**
2. Choose to **delete** your advertising ID entirely (Android allows this), or at minimum reset it and opt out of personalisation

---

Reduce What the Operating System Itself Collects

Your phone's maker collects "diagnostic" and "usage" data by default. You can reduce this.

On iPhone

1. **Settings → Privacy & Security → Analytics & Improvements** and turn off **Share iPhone Analytics**
2. Review **Settings → Privacy & Security → Apple Advertising** as above

Apple's business depends less on advertising than Google's, so an iPhone with these settings adjusted is reasonably private from third parties — though you remain within Apple's ecosystem.

On Android

Because Android is made by Google, a standard Android phone sends considerable data to Google in the background, and the settings only reduce — not eliminate — this. To genuinely remove Google from an Android phone requires replacing its operating system with a private, de-Googled one such as GrapheneOS. That is a substantial step covered in detail in the companion *Escaping Google* guide, which walks through the three levels of de-Googling a phone — from locking down your existing phone, through to installing GrapheneOS on a Pixel. If full phone de-Googling is your goal, that guide is where to do it properly. For now, to reduce what your current Android phone sends to Google:

1. **Settings → Google** → review and turn off **Web & App Activity**, **Location History**, and ad personalisation in your Google account settings

2. **Settings → Privacy** and turn off **Usage & diagnostics**
3. Go through the permission and advertising steps above

Manage Location Carefully

Location is among the most sensitive data your phone generates. Beyond per-app permissions:

- Turn off location entirely when you do not need it — a quick toggle in your phone's control panel
- On Android, in your Google account, turn off **Location History** (also called Timeline) so your movements are not continuously recorded and stored
- On iPhone, review **Settings → Privacy & Security → Location Services → System Services** and turn off the many background location uses you do not need, such as location-based suggestions and ads

---

Audit and Remove Apps You Do Not Use

Every app on your phone is a potential collector of your data. Apps you installed once and forgot may still be running, still collecting, still sending data.

1. Go through your installed apps
2. Delete any you do not actively use — this is one of the simplest and most effective privacy steps
3. For apps you keep, the fewer permissions they hold (from the steps above), the better

A lean phone with few apps, each tightly permissioned, leaks far less than a phone crowded with forgotten apps holding broad access.

Lock the Phone Itself

Privacy from companies matters, but so does protecting your phone from someone who physically picks it up.

- **Use a strong passcode**, not a four-digit PIN. A six-digit code at minimum; a longer alphanumeric one is better. Avoid obvious patterns and dates.
- **Enable biometric unlock** (fingerprint or face) for convenience, backed by the strong passcode
- **Make sure your phone is encrypted.** Modern iPhones are encrypted automatically when you set a passcode. Modern Android phones are generally encrypted by default. This protects your data if the phone is lost or stolen.
- **Set the screen to lock quickly** when idle
- **Review what is accessible from the lock screen** — consider disabling access to sensitive items (like message previews and the wallet) without unlocking first

---

A Note on Free Apps

A useful principle for phone privacy: if an app is free and you cannot see how the maker earns money, the answer is often that your data is the product. This does not mean free apps are all bad — many excellent privacy tools are free and funded by donations or paid tiers. But it is worth a moment's thought before installing a free app from an unfamiliar maker, especially one asking for broad permissions. Prefer reputable apps, open-source where possible, and apps whose business model does not depend on harvesting you.

Chapter Summary

Your phone holds the richest picture of your life, and by default shares much of it. Without replacing the phone, you can dramatically reduce this: the highest-impact step is auditing app permissions and ruthlessly revoking access apps do not need. Beyond that, turn off advertising tracking (App Tracking Transparency on iPhone, deleting the advertising ID on Android), reduce what the operating system collects, manage location carefully, delete unused

apps, and lock the phone itself with a strong passcode and encryption. An iPhone with these settings is reasonably private from third parties; a standard Android phone is improved but still reports to Google unless its operating system is replaced.

The next chapter goes after the companies that have built files on you behind your back: data brokers.

Chapter 7: Removing Yourself From Data Brokers →

CHAPTER 7

Removing Yourself From Data Brokers

The Industry That Profits From You

There is an entire industry most people have never heard of, built on collecting and selling your personal information. These companies are called **data brokers**, and there are hundreds of them. They assemble detailed files on nearly every adult — your full name, current and past addresses, phone numbers, email addresses, age, relatives and associates, estimated income, property records, court records, purchasing habits, and more.

You never signed up for this. They gather it from public records, from store loyalty programmes, from apps that sell your data, from other companies, and from each other. Then they sell it — to advertisers, to "people search" websites where anyone can look you up, to anyone willing to pay. If you have ever searched your own name and been unsettled to find a site listing your address and relatives, you have met a data broker.

This chapter is about getting your information off the market. It is one of the more laborious privacy tasks, but also one of the most concretely protective — especially against scammers, stalkers, identity thieves, and anyone who might wish to find you.

Why This Matters

The harms here are not abstract:

- **People-search sites** let anyone — an estranged relative, an angry stranger, a stalker — find your home address and phone number in seconds.
- **Scammers and identity thieves** buy broker data to make their scams convincing and to answer your security questions.
- **Spam and robocalls** are fed by brokered phone numbers and emails.
- **The profile compounds.** The more places your data sits, the more it spreads, because brokers sell to each other.

Removing yourself reduces all of these risks at once.

Two Approaches: By Hand or By Service

There are two ways to get your data removed, and the right choice depends on your time, your budget, and your threat model.

Approach One: Manual Removal (Free, But Laborious)

Every legitimate data broker is required to offer a way to opt out — to request removal of your information. You can do this yourself, for free, by going to each broker, finding their opt-out process, and submitting a request.

The reality of manual removal:

- There are *many* brokers — dozens of major ones and hundreds of smaller ones
- Each has its own opt-out process, some simple, some deliberately tedious
- The whole undertaking typically takes many hours spread over time
- Your data often reappears after months, requiring you to repeat the process
- It is free, and it gives you complete control, but it demands real persistence

How to approach it sanely:

- Start with the largest brokers, which feed many of the smaller ones — the big people-search sites are the priority
- Do a handful per session rather than attempting all at once; burnout is the main reason people quit
- Keep a record of which you have done and when, since you will need to check back
- Plan to repeat the major ones a couple of times a year

A useful free resource is the opt-out guidance maintained by the privacy community — sites like PrivacyGuides.org and others publish current, step-by-step opt-out instructions for individual brokers, since the processes change over time.

Approach Two: A Removal Service (Paid, But Hands-Off)

Because manual removal is so laborious and must be repeated, an industry of **data removal services** exists to do it for you. You sign up, give them permission to act on your behalf, and

they continuously send opt-out requests to hundreds of brokers and keep monitoring for your data reappearing.

The reality of removal services:

- They save you many hours and, crucially, they keep working continuously, re-removing your data when it reappears
- They cost money — typically a yearly subscription
- No service removes you from *everything* — none is 100% effective, and you should be wary of any that promises otherwise
- You are giving the service some of your information so they can find and remove it — so choosing a reputable one matters

Reputable services (always check current pricing and coverage before choosing, as these change frequently — the figures below are approximate as of 2026):

- **Incogni** — Widely regarded as a strong, affordable, automated option covering 420+ brokers with continuous monitoring; around $8/month billed annually
- **DeleteMe** — One of the longest-established services, using a mix of human researchers and automation; around $129/year
- **Optery** — Offers a genuinely useful *free scan* to show you where your data appears, with paid tiers (starting around $39/year) for removal; provides screenshot proof of removals
- **Privacy Bee**, **Kanary**, and others also operate in this space

Two important cautions before choosing a service:

- **No service removes you from everything, ever.** Be deeply skeptical of any service promising complete or permanent removal — it is not possible. They cover a finite list of known brokers, new brokers constantly appear, and data reappears. A good service meaningfully *reduces and suppresses* your exposure; it does not erase you.
- **You are giving the service your personal information.** To find and remove your data, a removal service necessarily needs to know who you are and what to look for — your name, addresses, and so on. This is a reasonable trade with a reputable, privacy-respecting company, but it means choosing one with a clean track record and a transparent privacy policy genuinely matters. You are trusting them with the very data you are trying to protect.

A practical tip: several of these offer a free scan that simply *shows* you where your information currently appears online. Even if you do not subscribe, running a free scan is an eye-opening way to see the scale of the problem and decide how to proceed.

Which Approach Is Right for You?

- If you have **time and patience** and want to spend nothing, **manual removal** works — focus on the big brokers and repeat periodically.
- If you have **a higher-risk situation** (an ex-partner you fear, a public-facing role, a stalking concern) or simply value your time, a **paid removal service** is worth the cost for the continuous, hands-off protection.
- A sensible **hybrid**: manually remove yourself from the handful of largest people-search sites right away (immediate protection from the most-used sites), and consider a service for the ongoing, comprehensive work.

Step 1: See Where You Are Exposed

Before removing anything, look at the scale of it:

1. Search your own name, in quotes, in a private search engine — add your city or state to narrow it
2. Note the people-search sites that list you (you will likely recognise several names that appear repeatedly)
3. Optionally, run a free scan from one of the removal services to get a fuller picture

This shows you what you are dealing with and gives you a starting list.

Step 2: Remove Yourself From the Largest Brokers First

Whether by hand or by choosing a service, prioritise the biggest people-search sites — the ones that appeared most prominently when you searched your name. These are the most-used and feed many smaller sites. Knocking these out gives the greatest immediate protection.

If doing it manually, find each site's opt-out or "remove my listing" page (often linked in the page footer or found by searching "[site name] opt out"), and follow their process.

Step 3: A Caution About Identity Verification

Some brokers ask you to verify your identity to process a removal — occasionally even requesting a photo of your government ID. Be careful here: you do not want to hand a data broker *more* sensitive information than they already have.

- Where possible, use opt-out methods that do not require ID
- If a broker insists on an ID and you choose to proceed, redact (black out) everything except the minimum needed — typically just your name and address — and consider writing "for opt-out purposes only" across the image
- A reputable removal service handles these situations using established channels, which is one of their advantages

---

Step 4: Monitor and Repeat

Data removal is not permanent. Brokers re-scrape public records and your data reappears over time.

- If doing it manually, set a reminder (in your private calendar) to recheck the major brokers every three to six months
- If using a service, this monitoring is done for you automatically — one of the main reasons people choose a service

---

A Realistic Expectation

You will not achieve perfect, total removal from every broker that exists — no one does, and any service claiming otherwise is overselling. What you *can* achieve is removal from the large, widely-used sites that pose the greatest risk, and ongoing suppression of your data so it stays far less available than it is now. That is a genuine and worthwhile reduction in your exposure to scammers, stalkers, and identity thieves.

A Word of Encouragement

This chapter describes the most tedious work in the whole guide — and if it feels daunting, that is completely understandable. So be kind to yourself about it: you do not have to do it all, or all at once. Removing yourself from even the five or six largest people-search sites — an afternoon's work, or a few minutes to start a service — already closes the doors that the overwhelming majority of snoops, scammers, and curious strangers would ever walk through. You do not need perfection here to be far safer than you are today. Do a little, breathe, and come back to it later. Progress counts.

Chapter Summary

Data brokers are a hidden industry that assembles and sells detailed files on nearly everyone, feeding people-search sites, scammers, and spam. You can remove yourself either manually (free but laborious, requiring repetition) or through a paid removal service like Incogni, DeleteMe, or Optery (hands-off and continuous, but costing money and never 100% complete). Start by searching your own name to see your exposure, prioritise the largest people-search sites, be cautious about handing over ID to verify removals, and monitor and repeat — or let a service do that for you. Perfect removal is impossible, but meaningfully reducing your exposure is very achievable.

The next chapter addresses the information you may be exposing yourself, often without realising: social media.

Chapter 8: Social Media Privacy →

CHAPTER 8

Social Media Privacy

The Information You Hand Over Willingly

Most of this guide is about information taken from you without your full awareness. Social media is different: it is information you hand over willingly, often enthusiastically — and that makes it both easier and harder to address. Easier, because you control what you post. Harder, because the entire design of these platforms encourages you to reveal more, and because what you have already shared may stretch back years.

This chapter is not necessarily about deleting your social media (though that is an option). It is about using it more privately — understanding what you expose, tightening who can see it, and reducing how much these platforms profile you.

What Social Media Knows and Does

Social media platforms — Facebook, Instagram, X, TikTok, LinkedIn, and the rest — are, like Google, mostly advertising businesses. Their profits come from understanding you well enough to sell your attention to advertisers. To do that, they collect far more than what you post:

- **Everything you post, like, comment on, and linger on** — building a detailed picture of your interests, beliefs, relationships, and emotional triggers
- **Your social graph** — everyone you are connected to, which reveals your family, friends, colleagues, and associations
- **Your activity off the platform** — through tracking code (like the Facebook "pixel") embedded across millions of other websites and apps, these platforms follow you even when you are not using them
- **Metadata about your posts** — including, often, the location where photos were taken
- **What you type but do not post** — some platforms record even drafts you abandon

And what you post publicly is available not just to the platform but to anyone — including employers, strangers, scammers, and the data brokers from the previous chapter, who harvest social media for their files.

The Two Privacy Problems

There are two distinct things to address, and they call for different actions:

1. **What other people can see** — your audience. This is controlled by the platform's privacy settings: who can see your posts, your profile, your friend list, your photos.
2. **What the platform itself collects and does with your data** — including its tracking of you across the rest of the web. This is controlled by a different set of settings, and by your broader habits.

We will address both.

Step 1: Lock Down Who Can See You

Go through the privacy settings of each social media account you use. The specifics differ by platform and change often, but the principles are the same everywhere. Look for and adjust:

- **Who can see your posts** — set to friends/connections only, rather than public, unless you have a reason to be public
- **Who can see your friends/connections list** — restrict this; your social graph is revealing and is used by others to map your relationships
- **Who can see your photos and tagged photos** — restrict, and review tagging permissions so you approve tags before they appear
- **Profile information** — remove or hide your phone number, email, birthday, hometown, workplace, and address. These are gold for scammers and data brokers. Ask yourself for each field: does this need to be visible to anyone, let alone everyone?
- **Search and discoverability** — limit whether you can be found by your phone number or email, and whether search engines can link to your profile
- **Location** — turn off location tagging on posts

A good rule: set everything to the most private option, then loosen only what you have a specific reason to share.

Step 2: Reduce the Platform's Tracking of You

Separately from your audience settings, look for privacy or ad settings that control the platform's own data use:

- **Off-platform activity tracking** — Facebook, for instance, has a setting (often called "Off-Facebook Activity" or similar) that shows and lets you disconnect the record of your activity on other websites and apps that has been linked to your account. Clear it and turn it off.
- **Ad personalisation** — turn off personalised ads where the platform allows, and remove interest categories it has assigned you
- **Data sharing with partners** — opt out of data sharing with third parties wherever offered
- **Facial recognition** — turn it off if the platform offers it

---

Step 3: Reconsider What You Post Going Forward

Settings help, but habits matter more. A few principles for posting more privately:

- **Assume anything you post could become public**, regardless of settings — settings change, accounts get breached, friends screenshot. Post accordingly.
- **Be cautious with location and travel.** Posting that you are on holiday tells the world your home is empty. Posting your location in real time tells people exactly where you are. Consider posting travel photos after you return.
- **Protect others, especially children.** Think carefully before posting photos of children — yours or others' — and the personal details of family and friends. They did not consent to the exposure.
- **Watch the background.** Photos can reveal more than intended — documents on a desk, a house number, a vehicle plate, a school uniform, the view from a window that pinpoints your location.
- **Strip photo location data.** As covered earlier in the series, photos can carry the GPS coordinates where they were taken. Many platforms remove this on upload, but not all — be mindful.
- **Decline the quizzes and "fun" data grabs.** Those "which character are you" quizzes and apps that want access to your profile are frequently data-harvesting operations. The

questions that mimic security questions (“your first pet, your street name”) are especially dangerous.

Step 4: Clean Up Your Past

Years of posts may sit on your accounts, revealing far more than you would share today.

- Most platforms let you download an archive of everything you have posted — worth doing both to see what is there and to keep your own copy
- Many platforms offer tools to bulk-delete or archive old posts, or to limit the audience of past posts in one action (Facebook, for example, has an option to limit all past public posts to friends)
- Review and remove old photos, posts, and personal details that no longer serve you
- Check which third-party apps you have connected to your social accounts over the years, and remove any you no longer use — each is a data pathway and a security risk

---

Step 5: Consider Your Overall Footprint

Beyond settings, it is worth asking bigger questions about each platform:

- **Do you still use it?** Dormant accounts are pure liability — they hold your data, can be breached, and keep profiling you. Deleting accounts you no longer use is a clean privacy win.
- **Could you use it more deliberately?** Some people keep a single platform for genuine connection and shed the rest. Others move to more private alternatives — for example, the privacy-respecting, advertising-free social networks built on open protocols (such as Mastodon and similar) that have grown in recent years.
- **Could you separate identities?** For platforms you use publicly (say, for work), keeping them strictly separate from your private life — different accounts, different information — limits how much one exposes the other.

There is no single right answer. The point is to use social media intentionally, rather than letting it use you by default.

A Balanced Note

Social media is not only a privacy hazard — it is also how many people stay connected to family, community, and the wider world, and that connection has real value. The goal of this chapter is not to shame anyone into deleting everything. It is to help you make conscious choices: to know what you are exposing, to tighten what does not need to be open, and to keep the genuine benefits while shedding the unnecessary risks. Even applying just the audience settings and turning off off-platform tracking puts you far ahead of where most people stand.

Chapter Summary

Social media is information you hand over willingly, on platforms designed to draw out more and to profile you — including tracking you across the rest of the web. Address it in two parts: lock down *who can see you* (set posts, friend lists, photos, and profile details to private, and hide personal information like phone, address, and birthday), and reduce *what the platform collects* (turn off off-platform activity tracking and ad personalisation). Going forward, post with the assumption it could become public, protect location and others' privacy, and avoid data-grab quizzes. Clean up years of past posts, remove unused connected apps, and consider deleting dormant accounts entirely. The aim is intentional use, keeping the genuine benefits while shedding unnecessary exposure.

The next chapter protects an area people rarely connect to privacy but which reveals enormous amounts about them: their money.

Chapter 9: Financial Privacy →

CHAPTER 9

Financial Privacy

What Your Spending Reveals

Your financial transactions are one of the most revealing records of your life. Where you shop, what you buy, where you eat, what you subscribe to, where you travel, which doctor or pharmacy you visit, what charities and causes you support, even your habits and vices — all of it is written in your spending. A complete record of someone's purchases is, in many ways, a complete record of their life.

This information is collected and used far more than most people realise. This chapter covers practical ways to keep your financial life more private — both from commercial data collection and from the more serious risks of fraud and theft.

An important clarification before we begin. This chapter is about legitimate financial *privacy* — your lawful right to keep your ordinary spending from being harvested, profiled, and sold by companies. It is emphatically *not* about evading taxes, hiding income, laundering money, or concealing anything from authorities to whom you are lawfully accountable, all of which are crimes and none of which this guide endorses or assists. Keeping your grocery purchases out of an advertising database and meeting your legal obligations are entirely compatible. Everything in this chapter is the former: normal, lawful privacy that any honest person is entitled to.

Who Sees Your Spending, and Why

Card networks and banks record every transaction and, in many cases, share or sell anonymised (and sometimes not-so-anonymised) spending data. Aggregated purchase data is a valuable commodity.

Payment apps — the popular peer-to-peer payment services — often have surprisingly public defaults. Some make your transactions visible to others unless you change the settings, exposing who you pay and sometimes why.

Retailers and loyalty programmes build detailed profiles of your purchases, tied to your identity through loyalty cards, and frequently sell or share this data. The famous examples of stores predicting major life events from shopping patterns are real.

Data brokers (from the earlier chapter) incorporate financial and purchase data into their profiles.

The more serious risks are fraud and identity theft: criminals who obtain your card details or enough personal information to open accounts in your name.

Step 1: Lock Down Your Payment Apps

This is the quickest, highest-impact financial privacy fix, because the defaults are often genuinely exposing.

The popular peer-to-peer payment apps sometimes default to making your transactions *visible* — to friends, or even publicly. Someone could potentially see who you pay and when.

1. Open each payment app you use
2. Find the privacy settings
3. Set all transactions to **private** (visible only to you)
4. Change the default for future transactions to private as well
5. Review your past transaction history visibility

Do this today if you use these apps — it takes two minutes and closes a surprisingly wide window.

Step 2: Use Virtual Card Numbers

One of the most powerful financial privacy and security tools is the **virtual card number** — a feature increasingly offered by banks and dedicated services. A virtual card is a card number linked to your real account but distinct from it, which you can create, limit, and cancel at will.

Why virtual cards are so useful:

- **They protect your real card number.** The merchant never sees your actual card details, so a breach at that merchant cannot expose your real card.
- **They can be locked to one merchant.** A virtual card tied to a single merchant is useless to a thief even if stolen, because it only works for that one merchant.
- **They can have spending limits.** You can cap the amount, which is ideal for subscriptions and trials.
- **They can be cancelled instantly.** If a merchant starts overcharging, or a free trial tries to convert, you simply delete that card — no calling the bank, no changing your real card.
- **They limit subscription traps.** Merchants cannot keep charging a card you have deleted.

How to get them:

- Check whether your bank offers virtual cards — many now do, built into their app, at no cost
- Dedicated services such as **Privacy.com** (in the United States) specialise in exactly this, letting you generate merchant-locked, limit-capped virtual cards easily; availability and features vary by country, so check what is offered where you live
- Some privacy-focused financial services and certain credit cards include the feature
- Availability differs significantly by country — virtual cards are widespread in some places and limited in others, so check what your own bank and local services provide

Using a fresh virtual card per merchant also has a privacy benefit similar to email aliases: it makes it harder to link your purchases across merchants into a single profile.

Step 3: Be Deliberate About Loyalty Programmes

Loyalty and rewards programmes are explicit trades: discounts in exchange for a detailed record of everything you buy, tied to your identity. That is a legitimate trade if you choose it knowingly — but choose it knowingly.

- Decide which programmes are genuinely worth the data you give up
- For programmes you use, consider whether you must attach your real phone number and email, or whether an alias email and minimal information suffice
- Some people maintain a loyalty account with deliberately minimal personal details

- Paying with a virtual card and providing an alias email keeps even a loyalty programme from linking cleanly to the rest of your profile

---

Step 4: Protect Against Fraud and Identity Theft

The more serious financial risks deserve direct attention.

Freeze your credit. This is one of the most powerful and underused protections. A credit freeze prevents anyone — including criminals — from opening new credit in your name, because lenders cannot access your credit file to approve a new account. It is free, it does not affect your existing accounts or your credit score, and you can temporarily lift it when you yourself need to apply for credit. In many countries you freeze your credit by contacting each of the major credit bureaus. For most people who are not frequently opening new accounts, keeping credit frozen by default is excellent protection against identity theft.

Monitor your accounts. Set up transaction alerts in your banking app so you are notified of charges. Review statements regularly. The sooner you catch fraud, the easier it is to resolve.

Use credit, not debit, for everyday purchases where possible. Credit cards generally offer stronger fraud protection than debit cards, and crucially, fraud on a credit card is the bank's money at risk until resolved, whereas debit fraud is *your* money out of your account while you sort it out.

Be alert to phishing. Many financial crimes start with a convincing fake email, text, or call designed to trick you into revealing details or passwords. Treat unexpected messages about your accounts with suspicion, never click links in them, and contact your bank directly using a number you look up yourself.

Step 5: Cash and Its Quiet Virtues

It is worth remembering the most private payment method of all: **cash**. Cash leaves no digital trail, builds no profile, and cannot be breached. Using cash for some everyday purchases — where practical — is a simple, legitimate way to keep a portion of your spending entirely private. As societies move toward cashless payment, the privacy value of cash only grows.

This is not about hiding anything; it is simply that not every coffee or newspaper needs to be recorded in a database.

A Note on Cryptocurrency

Cryptocurrency is sometimes promoted as a privacy tool for payments. The reality is nuanced. Most well-known cryptocurrencies, such as Bitcoin, are actually *less* private than a bank account in one important way: their transactions are recorded on a permanent public ledger that anyone can examine. While the addresses are not automatically tied to your name, they can often be linked back to you, and once linked, your entire transaction history is exposed forever. Certain specialised cryptocurrencies are designed for genuine privacy, but using any cryptocurrency safely and privately requires real knowledge and care, and it carries its own risks. For most people seeking everyday financial privacy, the practical tools in this chapter — payment-app settings, virtual cards, credit freezes, and cash — deliver far more benefit with far less complexity. Cryptocurrency is a deep topic best approached through dedicated, careful study rather than as a casual privacy fix.

A Word of Reassurance

Money can feel like the most intimidating area to take control of, but notice how much of this chapter is genuinely quick: setting a payment app to private takes two minutes, freezing your credit is free and done once, and turning on transaction alerts is a single setting. You do not have to overhaul your financial life — a few small, lawful changes meaningfully reduce both the profiling of your spending and your exposure to fraud. Start with the payment-app setting today, and add the rest when you are ready.

Chapter Summary

Your spending is one of the most revealing records of your life, collected by banks, payment apps, retailers, and data brokers, with fraud and identity theft as the more serious risks. The highest-impact quick fix is setting your peer-to-peer payment apps to private, since their defaults often expose your transactions. Virtual card numbers protect your real card, lock to

single merchants, and stop subscription traps. Be deliberate about loyalty programmes, and protect against fraud by freezing your credit (free and powerful), monitoring accounts, favouring credit over debit, and staying alert to phishing. Cash remains the most private payment method, and cryptocurrency is more nuanced than its reputation suggests. This is all legitimate financial privacy, which is your right.

The next chapter addresses the growing number of internet-connected devices in your home.

Chapter 10: Smart Devices and the Connected Home →

CHAPTER 10

Smart Devices and the Connected Home

The Listeners in Your Living Room

A generation ago, the objects in your home were just objects. Your television showed programmes. Your thermostat set the temperature. Your doorbell rang. Today, many of these same objects are "smart" — connected to the internet, equipped with microphones, cameras, and sensors, and continuously sending information back to the companies that made them.

This is the **Internet of Things** — the web of connected devices that now fills many homes: smart TVs, voice assistants, video doorbells, security cameras, smart speakers, connected thermostats, fitness trackers, even connected appliances. Each adds convenience. Each also potentially watches, listens, or records, and reports back. This chapter helps you enjoy the convenience while limiting the surveillance.

What Smart Devices Actually Collect

The collection is often far broader than the device's function suggests:

Smart TVs are among the worst offenders. Many use a technology that identifies everything you watch — including from external devices and even DVDs — and report your viewing back to the manufacturer and advertisers. Some have microphones and cameras. Your television may be watching you as much as you are watching it.

Voice assistants and smart speakers listen for their wake word, which means a microphone is always active in your home. Recordings of your requests — and sometimes accidental recordings — are sent to the company, stored, and in documented cases have been reviewed by human workers.

Video doorbells and security cameras record video and audio, often store it on the company's servers, and in some cases have shared footage with third parties, including law enforcement, sometimes without a warrant.

Fitness trackers and smartwatches collect intimate health and location data — your heart rate, sleep, movements, and continuous location.

Connected appliances and sensors collect usage patterns that reveal when you are home, awake, and active.

The common thread: these devices generate data about the most intimate space in your life — your home — and send it to companies whose data practices you rarely see.

The Guiding Principle: Does It Need to Be Smart?

The single most useful question to ask before buying or connecting any smart device is: *do I actually need the smart features?*

Often the answer is no. A television is a perfectly good television without being connected to the internet. A doorbell can ring without uploading video to a company's servers. Many "smart" features add little real value while adding real surveillance. The most private smart device is the one you chose not to make smart in the first place.

This is not a call to reject all connected technology — some of it is genuinely useful. It is a call to be *deliberate*: to add connected devices because you truly want their benefits, not by default, and to understand the trade you are making.

Step 1: Tame Your Smart TV

Your television is often the biggest offender and one of the easiest to address.

- **Turn off the viewing-tracking feature.** Look in your TV's settings for options usually found under privacy, or named something like "viewing information," "interest-based advertising," or a branded term. Turn these off. This stops the TV from identifying and reporting everything you watch.
- **Decline or limit data collection** during setup and in settings
- **Consider not connecting the TV to the internet at all.** If you watch through a separate streaming device or box, your TV itself does not need internet access. A TV that is not online cannot phone home. You lose the built-in apps but keep your privacy.

- **Cover or disable any camera**, and check whether the microphone (for voice control) can be turned off if you do not use it

---

Step 2: Reconsider Always-Listening Voice Assistants

Voice assistants involve an always-active microphone in your home. Decide whether the convenience is worth it for you.

If you choose to keep one:

- **Review and delete your voice recordings.** The major voice assistants have settings (in their apps or account pages) to review stored recordings and delete them, and to turn off the saving of future recordings and human review. Do this.
- **Turn off the human-review options** where offered
- **Mute the microphone** when you are not using it — most smart speakers have a physical mute button
- **Be mindful of placement** — a microphone in a bedroom or private space hears more than one in a kitchen

If you decide the privacy cost is not worth it, removing the device entirely is a legitimate and clean choice.

Step 3: Handle Cameras and Doorbells Carefully

Connected cameras and video doorbells deserve particular care because they record video and audio, often of others as well as yourself.

- **Use strong, unique passwords and two-factor authentication** on these accounts especially — hijacked cameras are a real and disturbing problem
- **Understand where the footage is stored** — on the company's servers (where it may be accessed or shared) or locally on a device you control. Where possible, prefer cameras that store footage locally rather than in the company's cloud.
- **Review the company's record on sharing footage** with third parties and law enforcement, and the settings that control this

- **Point cameras only where needed**, and be mindful of recording neighbours, passers-by, or shared spaces, which raises both privacy and sometimes legal questions
- **Consider whether interior cameras are worth the risk** of being hijacked or accessed

---

Step 4: Network-Level Protections

A more advanced but powerful approach is to control these devices at the level of your home internet connection.

- **Separate your smart devices onto a guest network.** Most home routers let you create a separate guest Wi-Fi network. Putting your smart devices on a separate network from your phones and computers means that if a smart device is compromised, it cannot easily reach your more important devices. This is one of the most effective protections.
- **Review what is connected to your network.** Periodically check your router's list of connected devices so you know what is actually on your network.
- **Keep device software updated.** Smart devices receive security updates that fix vulnerabilities — apply them, and be wary of cheap devices from makers who never provide updates.
- **Change default passwords.** Many smart devices ship with default passwords that are publicly known. Always change them.
- **For the technically inclined**, network-wide ad-and-tracker blocking (such as a Pi-hole, a small device that blocks tracking across your whole network) can limit what all your devices send out. This is an enthusiast's tool but a powerful one.

Step 5: Be Deliberate About New Purchases

The easiest privacy decisions are made before you buy:

- Ask whether you need the smart features at all, or whether a simpler "dumb" version does the job
- Favour devices that store data locally rather than in the maker's cloud
- Favour makers with a genuine privacy reputation and a track record of security updates
- Be especially cautious with very cheap connected devices from unknown makers, which often have poor security and unclear data practices

- Read what data the device collects before buying, not after

---

A Realistic Note

You do not need to rip every connected device out of your home to meaningfully improve your privacy. The biggest wins are simple: turn off your smart TV's viewing tracking, manage or remove always-listening assistants, secure your cameras properly, and put smart devices on a separate network. Even applying the first of these — taming the smart TV — closes one of the largest and least-known data leaks in the average home. As with everything in this guide, do what fits your life, and let the guiding question — *does it really need to be smart?* — steer your future choices.

Chapter Summary

The connected devices filling modern homes — smart TVs, voice assistants, cameras, doorbells, wearables — add convenience while potentially watching, listening, and reporting on the most intimate space in your life. The guiding question is whether a device needs to be smart at all. The highest-impact steps are taming your smart TV (turning off viewing tracking, or not connecting it at all), managing or removing always-listening voice assistants, securing cameras with strong passwords and local storage, and isolating smart devices on a separate guest network so a compromise cannot spread. Be deliberate about new purchases, favouring local storage, reputable makers, and the simpler non-smart option when the smart features add little.

The final chapter brings everything together into habits that last.

Chapter 11: Putting It All Together →

CHAPTER 11

Putting It All Together

From Tasks to Habits

If you have worked through this guide, you have made a remarkable number of improvements: private messaging, a hardened browser, protected email with aliases, strong passwords and two-factor authentication, locked-down phone settings, removal from data brokers, tightened social media, financial privacy, and a more private home. That is a genuine transformation.

But privacy is not a project you complete once and forget. It is a state you maintain. The companies and systems that collect your data do not stop; new accounts accumulate, new devices arrive, settings reset after updates, and your data creeps back onto broker sites. This final chapter is about turning everything you have done into lasting habits, and giving you a simple framework to maintain your privacy with modest ongoing effort.

The good news: maintenance is far easier than the initial work. You have already done the hard part.

The Privacy Maintenance Routine

A little regular attention keeps your privacy strong. Here is a simple routine, organised by how often each task needs doing. Set reminders in your private calendar so you do not have to remember.

Ongoing (as you go about daily life)

- Use your password manager to generate a strong unique password for every new account
- Use an email alias for every new signup
- Use a private virtual card for new merchants and subscriptions where you can
- Check app permissions before granting them when you install something new
- Think before you post on social media, and before you connect a new smart device

Monthly (about fifteen minutes)

- Review your bank and card statements for anything unexpected
- Glance at which apps you have installed and delete any you no longer use
- Check that nothing has auto-installed or changed permissions after updates

Every three to six months (about an hour)

- Recheck the major data broker sites for your information and re-remove as needed (or confirm your removal service is working)
- Review your social media privacy settings, which platforms change frequently
- Update the passwords on your most important accounts, and run your password manager's checker for weak or reused passwords
- Check your email address on Have I Been Pwned to see if it has appeared in new breaches
- Review the privacy settings on your phone, since updates sometimes reset them

Once a year (an afternoon)

- Do a fuller review of your whole setup using the checklist below
- Delete accounts and services you no longer use
- Review and renew your understanding of your threat model — has anything in your life changed?
- Update your tools to current best practice (privacy tools evolve; see the resources below)

The Complete Privacy Checklist

Use this to see at a glance what you have done and what remains. Do not feel you must tick every box — remember your threat model, and do what fits your life. Each item is a real improvement on its own. *(This checklist is also provided as a standalone, printable appendix at the end of the guide — Appendix A — so you can keep it separately or print it out.)*

Communications

- ☐ Private messenger (Signal) installed and used for personal conversations
- ☐ Important contacts moved to private messaging

- [ ] Disappearing messages considered for sensitive chats

Browsing

- [ ] Private browser (Firefox or Brave) installed and set as default
- [ ] Firefox hardened (if using Firefox)
- [ ] uBlock Origin installed
- [ ] Private search engine (Brave Search or similar) set as default

Email

- [ ] Private email provider (Proton Mail or similar) in use for sensitive mail
- [ ] Email alias service set up
- [ ] Aliases used for new signups

Accounts

- [ ] Password manager set up with a strong master passphrase
- [ ] Important accounts given strong unique passwords
- [ ] Two-factor authentication on all important accounts via an authenticator app
- [ ] Backup codes saved in the password manager

Phone

- [ ] App permissions audited and minimised
- [ ] Advertising tracking turned off
- [ ] Location settings tightened
- [ ] Unused apps deleted
- [ ] Strong passcode and encryption confirmed

Data brokers

- [ ] Searched own name to assess exposure
- [ ] Removed from the largest people-search sites (or service engaged)
- [ ] Reminder set to recheck periodically

Social media

- [ ] Audience settings locked down (posts, friends list, photos, profile details)

- ☐ Off-platform activity tracking turned off
- ☐ Personal details (phone, address, birthday) hidden
- ☐ Old posts and unused connected apps cleaned up
- ☐ Dormant accounts deleted

Finances

- ☐ Payment apps set to private
- ☐ Virtual cards in use where possible
- ☐ Credit frozen (if appropriate to your situation)
- ☐ Transaction alerts enabled

Home

- ☐ Smart TV viewing tracking turned off
- ☐ Voice assistant recordings managed or device removed
- ☐ Cameras secured with strong passwords and 2FA
- ☐ Smart devices isolated on a guest network

The Principles to Carry Forward

Tools change. Companies rise and fall, settings move, new threats and new protections appear. But the underlying principles of digital privacy are durable. If you internalise these, you will make good decisions long after the specific instructions in this guide have aged:

Minimise what you share. The data never collected is the data that can never be leaked, sold, or used against you. Default to giving out less — less information on forms, fewer permissions to apps, fewer connected devices, fewer accounts.

Separate and compartmentalise. Different emails, aliases, and accounts for different purposes prevent your life from being assembled into one profile. Keep your contexts apart.

Prefer tools that do not profit from you. Favour services whose business model is *not* harvesting your data — paid services, non-profits, open-source tools, and companies that make their money honestly by charging for a product rather than selling you.

Assume persistence. Anything you post, send, or enter could last forever and could become public. Act accordingly, especially with anything sensitive.

Match effort to your threat model. Do not exhaust yourself chasing perfect privacy you do not need, and do not neglect protections you genuinely do. Be honest about your own situation and act accordingly.

Good and sustained beats perfect and abandoned. The privacy setup you actually maintain protects you far more than an elaborate one you give up on. Choose changes you can live with.

A Note on Bringing Others With You

Your privacy is not entirely in your own hands, because privacy is partly collective. When a friend uploads their contacts, your information goes with it. When a family member posts a photo of you with the location attached, your privacy is affected. When few people use private tools, those who do stand out.

This means one of the most valuable things you can do is help the people around you. Not by lecturing — few things are less persuasive — but by quiet example and gentle help. Set up Signal with your family. Show a friend how to lock down their phone. Help an older relative freeze their credit. Each person who adopts these habits makes the whole environment more private, including for you. Privacy grows stronger the more it is shared.

Resources to Stay Current

The privacy landscape changes, so a few trustworthy, independent resources are worth knowing:

PrivacyGuides.org (https://www.privacyguides.org) — The leading independent, community-driven resource for privacy tools and advice. Not commercially driven, rigorously maintained, and the best single place to check whether a tool is still recommended and to find current alternatives. If anything in this guide ages, check here first.

Electronic Frontier Foundation — Surveillance Self-Defense (https://ssd.eff.org) — From a respected non-profit defending digital rights, these are excellent, accessible explanations of privacy concepts and step-by-step techniques.

Have I Been Pwned (https://haveibeenpwned.com) — Enter your email to check whether it has appeared in known data breaches. Safe, free, and run by a respected security researcher.

Your tools' own help pages — each maintains clear, current support documentation:

- Signal: https://support.signal.org
- Proton: https://proton.me/support
- Bitwarden: https://bitwarden.com/help

The companion guides in this series — *Escaping Google* (for leaving Google specifically and full phone de-Googling) and the *Privacy Stack* guide (for a deep, technical, surveillance-resistant computer setup) build further on the foundation this guide provides.

A good habit: every six months or so, visit PrivacyGuides.org to confirm your tools are still well-regarded and to learn what has changed.

Conclusion: You Are in Control Again

You began this guide as most people live their digital lives — tracked across the web, your data bought and sold, your conversations exposed, your accounts vulnerable, your devices reporting on you, all by default and mostly without your awareness.

You have changed that. Your conversations are private. The web no longer follows you so freely. Your email is protected and your real address shielded behind aliases. Your accounts are locked down with strong unique passwords and a second factor. Your phone shares far less. Your information is being pulled off the data broker market. Your social media, your finances, and your home all expose less than they did. And most importantly, you understand *why* — which means you can maintain all of this and adapt it as the world changes.

You did not have to become a technical expert. You did not have to give up the conveniences of modern life. You did not have to do it all at once. You made deliberate choices, one at a time, and reclaimed meaningful control over your own information.

Privacy was never about hiding. It was always about control — the ordinary, healthy right to decide who knows what about you. That control is yours again. Keep it, maintain it, and share it with the people you care about.

This guide is published by ShannonGuides — Plain Language Series. shannonguides.com

— APPENDIX A

The Privacy Checklist

This is a standalone, printable version of the complete privacy checklist from Chapter 11. Use it to see at a glance what you have done and what remains, to print and keep, or to work through at your own pace.

Do not feel you must tick every box. Remember your threat model — what you are protecting and from whom — and do what fits your life. Each item is a real improvement on its own. The five items marked ★ are the "quick wins" that deliver the large majority of the benefit; if you do nothing else, do those.

Communications

- ☐ ★ Private messenger (Signal) installed and used for personal conversations
- ☐ Important contacts moved to private messaging
- ☐ Disappearing messages considered for sensitive chats

Browsing

- ☐ ★ Private browser (Firefox or Brave) installed and set as default
- ☐ Firefox hardened (if using Firefox)
- ☐ ★ uBlock Origin installed
- ☐ Private search engine (Brave Search or similar) set as default
- ☐ Reputable paid VPN considered for public Wi-Fi (never a free VPN)

Email

- ☐ Private email provider (Proton Mail or similar) in use for sensitive mail
- ☐ Email alias service set up
- ☐ Aliases used for new signups

Accounts

- ☐ ★ Password manager set up with a strong master passphrase
- ☐ Important accounts given strong unique passwords
- ☐ ★ Two-factor authentication on all important accounts via an authenticator app
- ☐ Backup codes saved in the password manager
- ☐ Authenticator app encrypted backup enabled (so a lost phone does not lock you out)

Phone

- ☐ ★ App permissions audited and minimised
- ☐ Advertising tracking turned off (App Tracking Transparency on iPhone)
- ☐ Location settings tightened
- ☐ Unused apps deleted
- ☐ Strong passcode and encryption confirmed
- ☐ (iPhone) Hide My Email and iCloud Private Relay considered

Data brokers

- ☐ Searched own name to assess exposure
- ☐ Removed from the largest people-search sites (or service engaged)
- ☐ Reminder set to recheck periodically

Social media

- ☐ Audience settings locked down (posts, friends list, photos, profile details)
- ☐ Off-platform activity tracking turned off
- ☐ Personal details (phone, address, birthday) hidden
- ☐ Old posts and unused connected apps cleaned up
- ☐ Dormant accounts deleted

Finances

- ☐ ★ Payment apps set to private
- ☐ Virtual cards in use where possible
- ☐ Credit frozen (if appropriate to your situation)
- ☐ Transaction alerts enabled

Home

- ☐ Smart TV viewing tracking turned off
- ☐ Voice assistant recordings managed or device removed
- ☐ Cameras secured with strong passwords and 2FA
- ☐ Smart devices isolated on a guest network

Maintenance Reminders

Monthly (~15 min): Review statements; delete unused apps; check for changed permissions after updates.

Every 3–6 months (~1 hour): Recheck data brokers; review social media settings; update important passwords and run the password manager's checker; check Have I Been Pwned; review phone privacy settings.

Yearly (an afternoon): Full review using this checklist; delete unused accounts; revisit your threat model; update tools to current best practice (check PrivacyGuides.org).

This checklist accompanies The Plain Language Guide to Digital Privacy. ShannonGuides — Plain Language Series — shannonguides.com